О схеме, реализующей квантовую хеш-функцию

И. Г. Зиннатуллин*

Представлен алгоритм для построения k-кубитной схемы квантового хеширования с d параметрами, где $k \geq 3$, $2^{k-2} < d \leq 2^{k-1}$. Получены оценки $N_1 \leq 2^{k-1} + 11k - 24$ и $N_2 \leq 2^{k-1} + 3k - 8$ на количества элементарных однокубитных гейтов и CNOT-гейтов соответственно. При $k \geq 5$ обе оценки меньше соответствующих оценок алгоритма Бергхольма и соавторов (2005) в том же базисе гейтов.

Ключевые слова: квантовое хеширование, квантовая схема.

1. Предварительные сведения

Конструкции квантовых хеш-функций в амплитудной и фазовой формах представлены в работе [1]. Рассматривается схема для их реализации на k кубитах с d параметрами, где $k \geq 3$, $2^{k-2} < d \leq 2^{k-1}$. Элементарными считаются однокубитные гейты X, H, R_y, R_z и двухкубитный CNOT-гейт. Через N_1 и N_2 обозначаются количества элементарных однокубитных гейтов и CNOT-гейтов соответственно.

2. Преобразование квантового состояния в базисное нулевое состояние

Алгоритм из работы [2] преобразует произвольное k-кубитное состояние в $|0\rangle^{\otimes k}$. Схема состоит из каскада равномерно управляемых однокубитных гейтов с $j = k-1, \ldots, 1$ управляющими кубитами и заключительного однокубитного гейта. После преобразований каждому j соответствует блок, в котором чередуются 2^j однокубитных гейтов и $2^j - 1$ CNOT-гейтов. Используем разложение Тейта-Брайана в форме $R_x R_y R_z$. Поворот R_x на целевом кубите коммутирует с CNOT-гейтом, поэтому он переносится через CNOT-гейт и объединяется со следующим однокубитным гейтом. Далее пересчитываются углы разложения для объединенного

* *Зиннатуллин Илнар Гумарович* — ассистент кафедры теоретической кибернетики ИВМиИТ КФУ, e-mail: ilngzinnatullin@kpfu.ru.

Zinnatullin Ilnar Gumarovich — Assistant Lecturer, Department of Theoretical Cybernetics, Institute of Computational Mathematics and Information Technologies, Kazan Federal University.

Опубликовано на условиях лицензии CC-BY 4.0
Published under CC-BY 4.0

гейта. Последний однокубитный гейт каждого блока и заключительный однокубитный гейт раскладываются в форме $R_zR_yR_z$. Левый множитель R_z можно убрать: на $|0\rangle$ он даёт глобальную фазу. В итоге получаем оценки $N_1 \le 2^{k+1} - 2$ и $N_2 \le 2^k - k - 1$.

3. Приготовление равномерной суперпозиции

Пусть $k \ge 2$ — число кубитов, $3 \le d \le 2^k$. Необходимо приготовить состояние $\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle$ из $|0\rangle^{\otimes k}$. Если $d = 2^r$, где $2 \le r \le k$, достаточно применить гейт H к r младшим кубитам. В этом случае $N_1 = r$ и $N_2 = 0$. Далее предполагаем, что d не является степенью двойки, и используем алгоритм из работы [3].

Запишем $d = \sum_{j=0}^{m} 2^{l_j}$, где $0 \le l_0 < \ldots < l_m \le k - 1$ и $m \ge 1$. Согласно [3], схема содержит m гейтов X, l_0 гейтов H, один гейт R_y, $m-1$ управляемых гейтов R_y и $l_m - l_0$ управляемых гейтов H. Управляемые гейты имеют управление по состоянию $|0\rangle$. Используя разложения для управляемых гейтов из [3, рис. 6], получаем оценки:

$$N_1 = m + l_0 + 1 + 4(m-1) + 6(l_m - l_0) = 5m + 6l_m - 5l_0 - 3,$$
$$N_2 = 2(m-1) + (l_m - l_0) = 2m + l_m - l_0 - 2.$$

Поскольку $l_m - l_0 = \sum_{j=0}^{m-1} (l_{j+1} - l_j) \ge m$, $l_m \le k - 1$ и $l_0 \ge 0$, то

$$N_1 \le 5(l_m - l_0) + 6l_m - 5l_0 - 3 = 11l_m - 10l_0 - 3 \le 11k - 14,$$
$$N_2 \le 2(l_m - l_0) + l_m - l_0 - 2 = 3l_m - 3l_0 - 2 \le 3k - 5.$$

Границы достигаются при $d = 2^k - 1$. Оценки справедливы и при $d = 2^r$.

4. Разложение равномерно управляемого поворота

Равномерно управляемый поворот $\mathrm{UCR}_a^n(\tilde{\theta})$ с n управляющими кубитами, где $a \in \{y, z\}$, $\tilde{\theta} = (\theta_0, \ldots, \theta_{2^n-1})^T \in \mathbb{R}^{2^n}$, при состоянии $|j\rangle$ управляющего регистра применяет $R_a(\theta_j)$ к целевому кубиту. Согласно [2], этот гейт раскладывается в чередующуюся последовательность 2^n однокубитных поворотов R_a и 2^n CNOT-гейтов. Таким образом, $N_1 = N_2 = 2^n$.

5. Реализация квантового хеширования

Пусть $q \ge 3$ — натуральное число, $\varepsilon \in (0, 1)$, а $S = (s_0, \ldots, s_{d-1})$ — упорядоченный набор элементов $\mathbb{Z}_q$, такой, что для любого $x \in \mathbb{Z}_q \setminus \{0\}$ выполняется $\frac{1}{d} \left| \sum_{j=0}^{d-1} e^{2\pi i s_j x/q} \right| \le \varepsilon$. Выбор S определяет криптографические

свойства. Согласно [1], такой набор можно выбрать с $d = O((\log_2 q)/\varepsilon^2)$. Пусть $n = \lceil \log_2 d \rceil$ и $k = n + 1$.

Квантовая хеш-функция $\psi : \mathbb{Z}_q \to (\mathcal{H}^2)^{\otimes k}$ определяется как $|\psi(x)\rangle = \frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle \otimes R_a(\theta_j) |\phi\rangle$, где $a = y$, $\phi = 0$ для амплитудной формы и $a = z$, $\phi = 1$ для фазовой формы, $\theta_j = 4\pi s_j x/q$. Если $d < 2^n$, определим $\theta_j = 0$ при $d \le j \le 2^n - 1$. Положим $\tilde{\theta} = (\theta_0, \ldots, \theta_{2^n-1})^T \in \mathbb{R}^{2^n}$. Для вычисления $|\psi(x)\rangle$ выполняются следующие шаги:

1. Из $|0\rangle^{\otimes k}$ подготавливается $|0\rangle^{\otimes n} \otimes |\phi\rangle$: при $|\phi\rangle = |1\rangle$ к целевому кубиту применяется гейт X.
2. На первых n кубитах приготавливается равномерная суперпозиция $\frac{1}{\sqrt{d}} \sum_{j=0}^{d-1} |j\rangle$ по алгоритму из раздела 3.
3. Применяется гейт $\mathrm{UCR}_a^n(\tilde{\theta})$ с первыми n управляющими кубитами. Используется разложение из раздела 4.

Суммируя оценки для этих шагов, получаем $N_1 \le 2^n + 11n - 14 + 1 = 2^n + 11n - 13$ и $N_2 \le 2^n + 3n - 5$.

Теорема 1. *Для описанной k-кубитной схемы при $k \ge 3$, $2^{k-2} < d \le 2^{k-1}$ выполняются оценки $N_1 \le 2^{k-1} + 11k - 24$ и $N_2 \le 2^{k-1} + 3k - 8$.*

Универсальную схему для приготовления $|\psi(x)\rangle$ из $|0\rangle^{\otimes k}$ можно получить обращением схемы из раздела 2: порядок гейтов меняется на обратный, а каждый гейт заменяется эрмитово сопряженным. При этом оценки $N_1 \le 2^{k+1} - 2$ и $N_2 \le 2^k - k - 1$ сохраняются. При $k \ge 5$ обе оценки из теоремы 1 меньше этих универсальных оценок.

6. Заключение

Представлен алгоритм для построения k-кубитной схемы квантового хеширования с d параметрами, где $k \ge 3$, $2^{k-2} < d \le 2^{k-1}$. Получены оценки $N_1 \le 2^{k-1} + 11k - 24$ и $N_2 \le 2^{k-1} + 3k - 8$. При $k \ge 5$ обе оценки меньше соответствующих оценок универсального алгоритма из [2] после описанного разложения однокубитных гейтов. Главные члены оценок N_1 и N_2 уменьшены в 4 и 2 раза соответственно.

Благодарности

Работа выполнена за счет предоставленного в 2026 году Фондом науки и технологий Республики Татарстан гранта на осуществление фундаментальных и поисковых исследований в научных и образовательных

организациях, предприятиях и организациях реального сектора экономики Республики Татарстан.

Список литературы

[1] F. Ablayev, K. Khadiev, A. Vasiliev, M. Ziiatdinov, "Theory and applications of quantum hashing", *Quantum Reports*, **7**:2 (2025), 24. DOI: 10.3390/quantum7020024.

[2] V. Bergholm, J. J. Vartiainen, M. Möttönen, M. M. Salomaa, "Quantum circuits with uniformly controlled one-qubit gates", *Phys. Rev. A*, **71**:5 (2005), 052330. DOI: 10.1103/PhysRevA.71.052330.

[3] A. Shukla, P. Vedula, "An efficient quantum algorithm for preparation of uniform quantum superposition states", *Quantum Information Processing*, **23**:2 (2024), 38. DOI: 10.1007/s11128-024-04258-4 .

Статья поступила 23 октября 2026 г.

On a Quantum Circuit Implementing a Quantum Hash Function

I. G. Zinnatullin

We present an algorithm for constructing a k-qubit quantum hashing circuit with d parameters, where $k \geq 3$ and $2^{k-2} < d \leq 2^{k-1}$. We obtain the bounds $N_1 \leq 2^{k-1}+11k-24$ and $N_2 \leq 2^{k-1}+3k-8$ on the numbers of elementary one-qubit gates and CNOT gates, respectively. For $k \geq 5$, both bounds are lower than the corresponding bounds for the algorithm of Bergholm et al. (2005) in the same gate basis.

Keywords: quantum hashing, quantum circuit.

References

[1] F. Ablayev, K. Khadiev, A. Vasiliev, M. Ziiatdinov, "Theory and applications of quantum hashing", *Quantum Reports*, **7**:2 (2025), 24. DOI: 10.3390/quantum7020024.

[2] V. Bergholm, J. J. Vartiainen, M. Möttönen, M. M. Salomaa, "Quantum circuits with uniformly controlled one-qubit gates", *Phys. Rev. A*, **71**:5 (2005), 052330. DOI: 10.1103/PhysRevA.71.052330.

[3] A. Shukla, P. Vedula, "An efficient quantum algorithm for preparation of uniform quantum superposition states", *Quantum Information Processing*, **23**:2 (2024), 38. DOI: 10.1007/s11128-024-04258-4.

Received on October 23, 2026